Lecture 13

Tuesday, 10 January 2023 08:22

Sometimes, attacking the human is easier

social engineering → persuasion — whaling = CEO phishing

disgruntled employee

Elaboration Likelihood Model (ELM)

Routes to persuasion

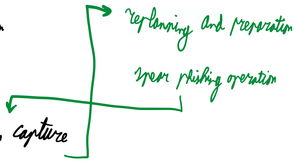
- central route
  - stimuli weighted by subject, final decision carefully elaborated
  - high amount of cognitive effort
  - careful elaboration of information
- peripheral route
  - no careful cognitive effort
  - convinced by unknowingly apparently relevant 'cues' which are actually unrelated
  - persuasion happens through 'adjacent clients'
    - likeability of subject
    - physical attractiveness
    - trust

Six weapons of human influence

social proof	peer pressure	you copy others' behavior
commitment		people prefer not to change their mind
reciprocation		people are nicer to nice people
liking	trusted people	you trust people (even if they do not have competences) whom you like
authority		
scarcity		people work for things that they'll lose something

social engineering steps

1. research and open source intelligence
2. planning and preparation
3. phishing operation
4. response and information capture
5. attack culmination & exploitation



---

advanced social engineering → generally targeted

impersonation

- address spoofer — wrong name
- name spoofer — wrong email
- previously owned attacker — wrong name + email
- lateral attacker — use actual identity of spoofed victim

attack is more effective when correct and spoofed domain are similar

DKIM: mail signed with key in possession of allowed mail service

SPF: sender policy framework, 'list' of authorized IP addresses
DMARC: pass, quarantine, reject mail which passes/fails DKIM/SPF

SPF, DKIM, DMARC only help against address spoofer

most often, malicious email comes from impersonated high-ranking individuals

context is relevant to success probability of phishing email

targeted phishing achieves effects (i.e. clicking) in hours

→ key bladder "very soon" is not a problem, victims already fell for it